Department of Commerce
Innovation is in our nature.

Administrative Requirements

FOR

Housing and Essential Needs Grant

Funded through the
Housing Assistance Unit
Community Services and Housing Division

(page left intentionally blank)

Table of Contents

1. Overview

The Housing and Essential Needs Grant is one of three new programs created by Engrossed Senate House Bill 2082 that terminated the Disability Lifeline Program, which ended October 2011.

Grant Activities: Housing and Essential Needs Grant funds are limited to providing rental assistance, utility assistance and essential needs for Medical Care Services recipients whose eligibility is determined by the Department of Social and Health Services (DSHS).

Fund Sources: General Fund State appropriation to the Department of Commerce for 2011-13 biennium**.**

2. Purpose

The purpose of the *Administrative Requirements* is to:

1. Establish the administrative and system requirements for Lead Grantees and Sub Grantees; and

2. Provide standards for such items as Sub Grantee Agreements and Reports.

This document is incorporated into Commerce's Housing and Essential Needs grant agreement and may be modified at any time during the grant period.

3. Eligible Lead Grantees

Local Governments and community based organizations.

Monitoring of Lead Grantee by Commerce

Commerce will monitor Lead Grantees grant activities. Lead Grantees will be given a minimum of 30 days notice unless there are special circumstances that require immediate attention.

Specific details of what will be reviewed and what materials the Lead Grantee will be required to submit will be outlined in the 30 day notice.

4. Sub Grantee Selection and Monitoring

Sub Grantee Selection

Lead Grantees applying for grant funds may enter into an agreement with any other local government, Council of Governments, Housing Authority, Community Action Agency, Regional Support Network (under 71.24 RCW), nonprofit community or neighborhood-based organization, federally recognized Indian tribe in the state of Washington, or regional or statewide nonprofit housing assistance organizations who execute programs to end homelessness within a defined service area. These entities shall be known as Sub Grantees.

All Sub Grantee agreements must be time limited and pass on all obligations and requirements mandated by Commerce, have defined roles and responsibilities for each party covered by the agreement, detailed budgets and performance terms, and be filed with Commerce within 60 days of grant execution. The grant *General Terms & Conditions* identify minimum sub contracting requirements. (Commerce reserves the right to directly contact Sub Grantees at any time for data quality, monitoring, fiscal and other issues.)

Lead Grantees must have sub grantee policies and/or procedures that at a minimum address the following:

1. Sub grantee solicitation and selection (must be submitted with Application)
2. Contract development (amendments)
3. Reimbursement (due dates, frequency, HMIS reports, documentation required)
4. Monitoring (notice, type, frequency, report format and content, consequences)
5. Termination (notice)

Sub Grantee Monitoring

1. The Lead Grantee shall conduct a risk assessment of Sub Grantees (at a minimum of every two years) and provide a Sub Grantee monitoring plan and schedule to Commerce within 120 days of grant execution.

2. Monitoring of Sub Grantees may consist of on-site or remote techniques and can be individualized based on results of the risk assessment or the number of Sub Grantees within the defined service area according to the Lead Grantee's monitoring policies and/or procedures. Commerce reserves the right to require Lead Grantees to undertake special reviews when an audit or other emerging issue demands prompt intervention and/or investigation.

If the Lead Grantee passes through grant funds to a Sub Grantee to administer the grant, the Lead Grantee must still monitor the Sub Grantee. The Lead Grantee must have a written agreement with the Sub Grantee that addresses the roles and responsibilities of monitoring.

5. Billing Procedures and Financial Records

Lead Grantees must bill Commerce on a monthly or quarterly basis for reimbursement of allowable costs, using a *Commerce Voucher Distribution Form*. Exceptions to the single billing per month (or quarterly) can be made by Commerce on a case-by-case basis. Invoices are due on the 20th of month/month's quarter following the provision of services. (Final invoices for a biennium may be due sooner than the 20th for the final report month.) If the Lead Grantee fails to file an invoice within a three-month period, without a reasonable explanation, Commerce will suspend payments, notify the Lead Grantee and take follow-up action that may include terminating the grant agreement.

Vouchers must include a client data report(s) generated by the Lead/Sub Grantees Homeless Management Information System (HMIS) with each submission. Commerce will create the template report.

Commerce also accepts electronic copies of signed A-19/invoices. This could be an emailed PDF or FAX of a signed A-19/invoice requesting reimbursement.

An electronic copy is the preferred method for requesting reimbursement, and will likely result in faster payment. You still have the option of mailing a printed/signed copy of the A-19/invoice, but please only send it electronically **or** by mail, not both.

Back-up Documentation

Commerce may require a Lead Grantee to submit detailed information on charges per the grant budget categories or may require source documentation. Lead Grantees must retain on file the original invoice submitted by their Sub Grantee. Lead Grantees should have a clear contractual expectation with their Sub Grantee about what additional documentation is required for reimbursement.

6. Reporting

Agency Partner HMIS Agreement
All Lead/Sub Grantees must use HMIS for data collection and reporting purposes. Data must be collected in accordance with the Agency Partner HMIS Agreement (see Appendix B).

Daily, Monthly, Quarterly and Annual Reports to Stakeholders – Commerce will generate reports from the state data warehouse for reporting to all external stakeholders. Commerce will use the most updated federal HMIS Data Standards for all reports. Additional reporting needs in regards to fiscal management, monitoring activities, and other unforeseen report requests will be negotiated with Lead Grantees on an ongoing basis as needed and are expected to be minimal.

Data Quality Reports – Commerce will use the invoice process to ensure timely, accurate, and quality data is being entered into the state data warehouse (for specific required data for Lead/ Sub Grantees, please see **Appendix A** "Data Collection Directives"). Reimbursements to Lead Grantees will not be paid until data is accurate, timely and of high quality.

Data Sharing with DSHS – On a quarterly basis, identified data is shared with Research and Data Analysis at DSHS for further data analysis and reporting regarding cross-systems performance measures. Quarterly reports on cross-system analysis are posted on the Commerce website at commerce.wa.gov. Lead Grantees can expect an annual county level report via the data sharing agreement Commerce holds with DSHS~~.~~

Appendix A

Data Collection Directives

Client Records and Record Retention – Lead and Sub Grantees must enter a record for every client served with grant funds in the state homeless data warehouse (usually referred to as "HMIS") or in a local data collection system that meets HUD/HMIS data standards. The client record may contain personally identifying data or it may not, depending on whether the client provided informed, written consent to have their identifiers stored in HMIS. As a general rule, Commerce does not want personal identifiers for any client who identifies themselves as a victim of domestic violence, sexual assault, dating violence or stalking.

Agencies must develop and adopt policies governing the retention of paper records containing personally identifying information derived from a Homeless Management Information system. The policy must define how long paper records are retained after they are no longer being actively utilized, and the process that will be used to destroy the records to prevent the release of personally identifying information. The policy must require the destruction of the paper records derived from an HMIS no longer than seven years after the last day the person was served by the organization.

Funding Decisions & Data Collection – Lead Grantees must not make funding or resource allocation decisions of grant funds based on whether a Sub Grantee enters *personal identifiers* for victims of domestic violence, sexual assault, dating violence or stalking or other clients who have not provided informed, written consent. The intent of this guideline is to ensure that clients do not feel coerced into providing consent to share data at any time in any local jurisdiction receiving funds and participating in HMIS.

Data quality is of high concern for purposes of accurate reporting out of HMIS. Commerce recommends that local jurisdictions continue to strive for increased data quality including 1) monitoring completeness of required data elements and 2) monitoring responsible use of HMIS at local agencies. Some suggestions for how to appropriately include data quality in HMIS as a part of local funding decisions include, but are not limited to:

1) Completeness of required data elements:

    - Exclude clients who "refused consent" from the equation e.g.: Instead of $\frac{\text{\# NULL values}}{\text{All client records}}$ =% use $\frac{\text{\#NULL values}}{\text{Clients who DIDN'T refuse consent}}$ =%

2) Responsible use of HMIS at local agencies:

    - Develop a "baseline" rate of "refused consent" locally using HMIS data

- Determine each agency's rate of "refused consent" as a % deviation from the standard
- Add or subtract points for less or more deviation from the standard rate, depending on reasonableness

- Further training, technical assistance, or other guidance may be more appropriate in this situation instead of, or in addition to, penalties assessed during funding competitions

All local jurisdictions interested in including a measure of HMIS data quality as part of a local funding decision for funding are required to submit a proposal to Commerce for final approval prior to being used in local applications/competitions for funding.

Informed Consent – According to RCW 43.185C.180, personally identifying information about homeless individuals for the Washington homeless client management information system may only be collected after having obtained informed, reasonably time limited, (i) written consent from the homeless individual to whom the information relates, or (ii) telephonic consent from the homeless individual, provided that written consent is obtained at the first time the individual is physically present at an organization with access to the Washington homeless client management information system. Safeguards consistent with federal requirements on data collection must be in place to protect homeless individuals' right regarding their personally identifying information. Data collection under this subsection shall be done in a manner consistent with federally informed consent guidelines regarding human research which, at a minimum, require that individuals receive: (i) information about the expected duration of their participation in the Washington homeless client management information system; (ii) an explanation of whom to contact for answers to pertinent questions about the data collection and their rights regarding their personal identifying information; (iii) an explanation regarding whom to contact in the event of injury to the individual related to the Washington homeless client management information system; (iv) a description of any reasonably foreseeable risks to the homeless individual; and (v) a statement describing the extent to which confidentiality of records identifying the individual will be maintained.

Personal Identifiers – "Personally Identifying Data"— Individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, could include:

1. a first and last name;

2. a home or other physical address;

3. contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);

4. a social security number; and

5. any other information, including date of birth, racial or ethnic background, or religious affiliation that, in combination with any other non-personally identifying information, would serve to identify any individual collecting "non-identified" client records.

Data Entry for "Non-identified" Client Records

1. Leave the "Name" fields NULL (blank). Do not write in names ***such as "Anonymous" or "Refused" as that will compromise data quality at the state level.***

2. ***If there are no personal identifiers*** for a client record, there needs to be an "Agency Unique ID" of some sort created and stored in the system that can be used by the agency to access the record at a later time (and should not be an algorithm of elements that can lead to the client's identification).

3. Enter an approximate year of birth – subtract or add one to three years to the actual year of birth.

4. Enter "Refused" for gender, race, and ethnicity when the real answers to those questions, in combination with other data, can potentially lead to identification of the client.

5. Enter any additional answer to the universal, program-specific and optional data elements (from the March 2010 HMIS Data Standards) only if the answers to those questions, in combination with other data, will not lead to the identification of the client.

6. Program Entry Date, Program Exit Date and Service Date are generally required unless those elements can be used in combination with other elements to identify the client. If this is the case, please enter an approximate Program Entry Date, Program Exit Date and Service Date by adding one to three months to the actual dates and keeping the "Length of Stay" (the number of days between program entry and program exit) consistent with reality. Keeping the approximate service date, if used, within the actual service date's reporting period is also recommended.

Submitting data to the state data warehouse – If a Lead or Sub Grantee is not entering data directly into the state data warehouse, the data being entered into the local HMIS must be submitted on a quarterly basis no later than the 10th day following the end of each quarter to the state data warehouse via the HUD Standard 3.0 XML schema.

Appendix B

Agency Partner HMIS Agreement

The Homeless Management Information System ("HMIS") is a client management system that maintains information regarding the characteristics and service needs of Clients for a variety of reasons, including the provision of more effective and streamlined services to Clients and the creation of information that communities can use to determine the use and effectiveness of services.

Ultimately, when used correctly and faithfully by all involved parties, the HMIS is designed to benefit multiple stakeholders, including provider agencies, persons who are homeless, funders and the community through improved knowledge about people who are homeless, their services and service needs and a more effective and efficient service delivery system.

The Homeless Housing and Assistance Act of 2005 requires the Department of Commerce to collect HMIS data in the form of a data warehouse. Each homeless service provider will submit HMIS data to Commerce.

Agency and the Department of Commerce agree as follows:

1. General Understandings:

a. In this Agreement, the following terms will have the following meanings:

(i) "Client" refers to a consumer of services;

(ii) "Partner Agency" refers generally to any Agency participating in HMIS.

(iii) "Agency staff" refers to both paid employees and volunteers.

(iv) "HMIS" refers to the HMIS system administered by Commerce.

(v) "Enter(ing)" or "entry" refers to the entry of any Client information into HMIS.

(vi) "Shar(e)(ing)," or "Information Shar(e)(ing)" refers to the sharing of information which has been entered in HMIS with another Partner Agency.

(vii) "The Balance of State Continuum of Care Steering Committee" or "Steering Committee" refers to a Commerce advisory body that serves in a consultative and counseling capacity to Commerce as the system administrator. The Steering Committee is comprised of representatives from the State, the Balance of State Continuum of Care regions and at large members.

(viii) "Identified Information" refers to Client data that can be used to identify a specific Client. Also referred to as "Confidential" data or information.

(ix) "De-identified Information" refers to data that has specific Client demographic information removed, allowing use of the data ***without identifying*** a specific Client. Also referred to as "non-identifying" information.

b. Agency understands that when it enters information into HMIS, such information will be available to Commerce staff who may review the data to administer HMIS; to conduct analysis in partnership with the Research and Data Analysis (RDA) division at the Department of Social and Health Services (DSHS); and to prepare reports that may be submitted to others in de-identified form ***without*** individual identifying Client information.

c. Agency understands that Agency will have the ability to indicate whether information Agency entered into HMIS may be shared with and accessible to Partner Agencies in HMIS system. Agency is responsible for determining and designating in HMIS whether information may or may not be shared.

2. Confidentiality:

a. Agency will not:

(i) enter information into HMIS which it is not authorized to enter; and

(ii) will not designate information for sharing which Agency is not authorized to share, under any relevant federal, state, or local confidentiality laws, regulations or other restrictions applicable to Client information. By entering information into HMIS or designating it for sharing, Agency represents that it has the authority to enter such information or designate it for sharing.

b. If Agency is a "covered entity" whose disclosures are restricted under HIPAA (45 CFR 160 and 164) or is subject to Federal Drug and Alcohol Confidentiality Regulations (42 CFR Part 2), a fully executed Business Associate or Business Associate/Qualified Service Organization Agreement must be attached to this agreement before information may be entered. Sharing of information will not be permitted otherwise. More information about "covered entities" can be found here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.

c. If Agency is subject to any laws or requirements which restrict Agency's ability to either enter or authorize sharing of information, Agency will ensure that any entry it makes and all designations for sharing fully comply with all applicable laws or other restrictions.

d. Agency shall comply with the Violence Against Women and Department of Justice Reauthorization Act of 2005 (VAWA) and Washington State RCW 43.185C.030. No Identified Information may be entered into HMIS for Clients in licensed domestic violence programs or for Clients fleeing domestic violence situations.

e. To the extent that information entered by Agency into HMIS is or becomes subject to additional restrictions, Agency will immediately inform Commerce in writing of such restrictions.

3. Information Collection, Release and Sharing Consent:

a. **Collection of Client Identified information**: An agency shall collect client identified information only when appropriate to the purposes for which the information is obtained or when required by law. An Agency must collect client information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

b. **Obtaining Client Consent:** In obtaining Client consent, each adult Client in the household must sign the ***HMIS Client Release of Information*** (or a Commerce-approved equivalent release document) to indicate consent to enter Client identified information into HMIS. If minors are present in the household, at least one adult in the household must consent minors by writing their names on the ***HMIS Client Release of Information***. If any adult member of a household does not provide written consent, identifying information may not be entered into HMIS for *anyone* in the household. An unaccompanied youth may sign the consent form for themselves.

(i) Do not enter personally indentifying information into HMIS for clients who are in licensed domestic violence agencies or currently fleeing or in danger from a domestic violence, dating violence, sexual assault or stalking situation.

(ii) Telephonic consent from the individual may temporarily substitute written consent provided that written consent is obtained at the first time the individual is physically present at Agency.

(iii) A Client may withdraw or revoke consent for Client identified information collection by signing the ***HMIS Revocation of Consent***. If a Client revokes their consent, Agency is responsible for immediately contacting Commerce and making appropriate data modifications in HMIS to ensure that Client's personal identified information will not be shared with other Partner Agencies or visible to the Agency staff within the system.

(iv) This information is being gathered for the collection and maintenance of a research database and data repository. The consent is in effect until the client revokes the consent in writing.

(v) **No Conditioning of Services:** Agency will not condition any services upon or decline to provide any services to a Client based upon a Client's refusal to allow entry of identified information into HMIS.

(vi) **Re-release Prohibited:** Agency agrees not to release any Client identifying information received from HMIS to any other person or organization without written informed Client consent, or as required by law.

(vii) **Client Inspection/Correction:** Agency will allow a Client to inspect and obtain a copy of his/her own personal information except for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. Agency will also allow a Client to correct information that is inaccurate. Corrections may be made by way of a new entry that is in addition to but is not a replacement for an older entry.

c. **Security:** Agency will maintain security and confidentiality of HMIS information and is responsible for the actions of its users and for their training and supervision. Among the steps Agency will take to maintain security and confidentiality are:

d. **Access:** Agency will permit access to HMIS or information obtained from it only to authorized Agency staff who need access to HMIS for legitimate business purposes (such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements). Agency will limit the access of such staff to only those records that are immediately relevant to their work assignments.

e. **User Policy:** Prior to permitting any user to access HMIS, Agency will require the user to sign a ***User Policy, Responsibility Statement & Code of Ethics*** ("User Policy"), which is found on the Commerce web page (www.commerce.wa.gov/hmiswa) and is incorporated into this agreement and may be amended from time to time by Commerce. Agency will comply with, and enforce the User Policy and will inform Commerce immediately in writing of any breaches of the User Policy

f. **Computers:** Security for data maintained in HMIS depends on a secure computing environment. Computer security is adapted from relevant provisions of the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-01; see http://www.hud.gov/offices/cpd/homeless/hmis/standards/index.cfm). Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS.

Agency agrees to allow access to HMIS only from computers which are:

- owned by Agency or approved by Agency for the purpose of accessing and working with HMIS.
- protected from viruses by commercially available virus protection software.
- protected with a software or hardware firewall.
- maintained to insure that the computer operating system running the computer used for the HMIS is kept up to date in terms of security and other operating system patches, updates, and fixes.

- accessed through web browsers with 128-bit encryption (e.g., Internet Explorer, version 6.0). Some browsers have the capacity to remember passwords, so that the user does not need to type in the password when returning to password-protected sites. This default shall ***not*** be used with respect to Commerce' HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system.
- staffed at all times when in public areas. When computers are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should minimally include: logging off the data entry system, physically locking the computer in a secure area, or shutting down the computer entirely.

g. **Passwords:** Agency will permit access to HMIS only with use of a User ID and password, which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location.

Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, or the HMIS name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so long as the .default password is changed on first use. Passwords and user names shall be consistent with guidelines issued from time to time by HUD and/or Commerce.

h. **Training/Assistance:** Agency will permit access to HMIS only after the authorized user receives appropriate confidentiality training including that provided by Commerce. Agency will also conduct ongoing basic confidentiality training for all persons with access to HMIS and will train all persons who may receive information produced from HMIS on the confidentiality of such information. Agency will participate in such training as is provided from time to time by Commerce. Commerce will be reasonably available during Commerce defined weekday business hours for technical assistance (i.e. troubleshooting and report generation).

i. **Records:** Agency and Commerce will maintain records of any disclosures of Client identifying information either of them makes of HMIS information for a period of **seven** years after such disclosure. On written request of a Client, Agency and Commerce will provide an accounting of all such disclosures within the prior **seven-**year period. Commerce will have access to an audit trail from HMIS so as to produce an accounting of disclosures made from one Agency to another by way of sharing of information from HMIS.

j. **Retention of paper copies of personally identifying information:** Agencies must develop and adopt policies governing the retention of paper records containing personally identifying information derived from a Homeless Management Information system. The policy must define how long paper records are retained after they are no longer being actively utilized, and the process that will be used to destroy the records to prevent the release of personally identifying information. The policy must require the destruction of the paper records derived from an HMIS no longer than seven years after the last day the person was served by the organization.

4. Information Entry Standards:

a. Information entered into HMIS by Agency will be truthful, accurate and complete to the best of Agency's knowledge.

b. Agency will ***not*** solicit from Clients or enter information about Clients into the HMIS database unless the information is required for a legitimate business purpose such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements.

c. Agency will only enter information into HMIS database with respect to individuals that it serves or intends to serve, including through referral.

d. Agency will enter all data for a particular month into HMIS database by the 5th business day of the following month. Additionally, Agency will make every attempt enter all data for a particular week by the end of that week.

e. Agency will not alter or over-write information entered by another Agency.

5. Use of HMIS:

(i) Agency will not access identifying information for any individual for whom services are neither sought nor provided by the Agency. Agency may access identifying information of the Clients it serves and may request via writing access to statistical, non-identifying information on both the Clients it serves and Clients served by other HMIS participating agencies.

(ii) Agency may report non-identifying information to other entities for funding or planning purposes. Such non-identifying information shall not directly identify individual Clients.

(iii) Agency and Commerce will report only non-identifying information in response to requests for information from HMIS unless otherwise required by law.

(iv) Agency will use HMIS database for legitimate business purposes only.

(v) Agency will not use HMIS in violation of any federal or state law, including, but not limited to, copyright, trademark and trade secret laws, and laws prohibiting the transmission of material, which is threatening, harassing, or obscene.

(vi) Agency will not use the HMIS database to defraud federal, state or local governments, individuals or entities, or conduct any illegal activity.

6. Proprietary Rights of the HMIS:

(i) Agency shall not give or share assigned passwords and access codes for HMIS with any other Agency, business, or individual. Each user shall request their own login and password.

(ii) Agency shall take due diligence not to cause in any manner, or way, corruption of the HMIS database, and Agency agrees to be responsible for any damage it may cause.

(iii) **Steering Committee:** Commerce will consult with the Steering Committee from time to time regarding issues such as revision to the form of this Agreement. Written Agency complaints that are not resolved may be forwarded to the Steering Committee, which will try to reach a voluntary resolution of the complaint.

(iv) **Limitation of Liability and Indemnification:** No party to this Agreement shall assume any additional liability of any kind due to its execution of this agreement of participation in the HMIS. It is the intent of the parties that each party shall remain liable, to the extent provided by law, regarding its own acts and omissions; but that no party shall assume additional liability on its own behalf or liability for the acts of any other person or entity except for the acts and omissions of their own employees, volunteers, agents or contractors through participation in HMIS. The parties specifically agree that this agreement is for the benefit if the parties only and this agreement create no rights in any third party.

(v) **Limitation of Liability.** Commerce shall not be held liable to any member Agency for any cessation, delay or interruption of services, nor for any malfunction of hardware, software or equipment.

(vi) **Disclaimer of Warranties.** Commerce makes no warranties, express or implied, including the warranties or merchandise ability and fitness for a particular purpose, to any Agency or any other person or entity as to the services of the HMIS to any other matter.

Additional Terms and Conditions:

(vii) Agency will abide by such guidelines as are promulgated by HUD and/or Commerce from time to time regarding administration of the HMIS.

(viii) Agency and Commerce intend to abide by applicable law. Should any term of this agreement be inconsistent with applicable law, or should additional terms be required by applicable law, Agency and Commerce agree to modify the terms of this agreement so as to comply with applicable law.

(ix) Neither Commerce nor Agency will transfer or assign any rights or obligations regarding HMIS without the written consent of either party.

(x) Agency agrees to indemnify and hold Commerce and its agents and staffs harmless from all claims, damages, costs, and expenses, including legal fees and disbursements paid or incurred, arising form any breach of this Agreement or any of Agency's obligations under this Agreement.

(xi) This Agreement will be in force until terminated by either party. Either party may terminate this agreement at will with 20 days written notice. Either party may terminate this agreement immediately upon a material breach of this Agreement by the other party, including but not limited to the breach of the Commerce Security Policy by Agency.

(xii) If this Agreement is terminated, Agency will no longer have access to HMIS. Commerce and the remaining Partner Agencies will maintain their right to use all of the Client information previously entered by Agency except to the extent a restriction is imposed by Client or law.

(xiii) Copies of Agency data will be provided to the Agency upon written request of termination of this agreement. Data will be provided on CDs or other mutually agreed upon media. Unless otherwise specified in writing, copies of data will be delivered to Agency within fourteen (14) calendar days of receipt of written requests for data copies.

Appendix C

Data Security Requirements

The words and phrases listed below shall each have the following definitions:

"BVS" means the DSHS Benefit Verification System

"Data Provider" means the entity, Department of Social and Health Services

"Data Recipient" means the entity, Department of Commerce and its grantees which is receiving the Data from the Data Provider

Activity for which the Data is needed - to determine DSHS client eligibility for the Housing and Essential Needs Program

Description of Data - Housing Authority Profile will consist of the following BVS data elements:

Client ID Number

Client First Name

Client Middle Name

Client Last Name

Program Type

Household Number

DSHS Benefit

Earned Income

Unearned Income

Intentional Overpayment Amount

Potential HEN Eligibility

Data Access

Grantees shall access information using personal computers via an Internet connection using an SSL through Fortress 3 to access the DSHS BVS secure website.

Access to this website requires the user to have an e-mail address approved by DSHS. DSHS will provide the initial password and the strong password must be changed to a unique strong password.

Requirements for Access

Access to Data shall be limited to Grantees whose duties specifically require access to the Data in the performance of their assigned duties.

The Grantee shall provide Commerce with a list that contains the names of their staff that will need access to the Data.

The Grantee must immediately notify Commerce when any of their staff or Grantee staff with access to the Data is terminated from employment or when his or her job duties no longer require access to the Data.

Grantee's shall sign the Use and Disclosure requirements form each year and agree to adhere to the use and disclosure requirements.

The signed DSHS Notice of Nondisclosure forms shall be maintained by the Grantee and be submitted to Commerce upon request.

CONFIDENTIALITY AND NONDISCLOSURE

Grantees cannot disclose, transfer, or sell any such information to any party, except as provided by law or, in the case of Personal Information, without the prior written consent of the person to whom the Personal Information pertains

The Data to be shared is confidential in nature and is subject to state and federal confidentiality requirement that bind the Department of Commerce, its staff and their grantees and their staff to protect the confidentiality of the personal information contained in Economic Services Administration data.

Grantees shall maintain the confidentiality of personal data in accordance with state and federal laws, and shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements, including restrictions on re-disclosure.

Grantees shall take reasonable precautions to secure against unauthorized physical and electronic access to client data, which shall be protected in a manner that prevents unauthorized persons, including the general public, from retrieving data by means of computer, remote terminal, or other means.

1. **Data Transport.** When transporting DSHS Confidential Information electronically, including via email, the data will be protected by:

   a. Transporting the data within the (State Governmental Network) SGN or contractor's internal network, or;

   b. Encrypting any data that will be in transit outside the SGN or contractor's internal network. This includes transit over the public Internet.

2. **Protection of Data.** The Grantee agrees to store data on paper only, no electronic storage is allowable:

   a. **Paper documents.** Any paper records must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

3. **Data Disposition.** When the contracted work has been completed or when no longer needed, data shall be returned to DSHS or destroyed. Media on which data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	**Will be destroyed by:**
Paper documents with sensitive or confidential data	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of data will be protected.
Paper documents containing confidential information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Magnetic tape	Degaussing, incinerating or crosscut shredding

4. **Notification of Compromise or Potential Compromise**. The compromise or potential compromise of DSHS shared data must be reported to Commerce within one (1) business day of discovery.